(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 October 2001 (25.10.2001)

PCT

(10) International Publication Number
WO 01/78491 A3

(51) International Patent Classification[7]: H04L 9/00, 9/30

(21) International Application Number: PCT/US01/12157

(22) International Filing Date: 12 April 2001 (12.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/549,446 14 April 2000 (14.04.2000) US

(71) Applicant: POSTX CORPORATION [US/US]; 3 Results Way, Cupertino, CA 95014 (US).

(72) Inventors: VENKATRAMAN, Rajamadam, C.; 1031 Harlan Drive, San Jose, CA 95129 (US). SAHASRABAUDDHE, Unmesh; 875 University Avenue #5, Palo Alto, CA 94301 (US). SHORT, Steven; 786 Bend Avenue, San Jose, CA 95136 (US). WARTY, Ashish; 1818 Canal Way, San Jose, CA 95132 (US).

(74) Agents: JAKOPIN, David, A. et al.; Pillsbury Winthrop LLP, 1600 Tysons Boulevard, McLean, VA 22102 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
14 March 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/78491 A3

(54) Title: SYSTEMS AND METHODS FOR ENCRYPTING/DECRYPTING DATA USING A BROKER AGENT

(57) Abstract: The present invention relates to systems and methods for providing secure symmetric and asymmetric encryption/decryption using an intermediate or broker agent. The broker agent (i.e., a server) is used to encrypt and decrypt data and/or session key during the transmission of the data from the sender to the recipient. These encryption processes are more secure because the recipients do not have access to the sender's private and public keys. The first and second embodiment relate to symmetric encryption/decryption systems and methods, while the third and fourth embodiments relate to asymmetric encryption/decryption systems and methods.

DF

INTERNATIONAL SEARCH REPORT

Im tional Application No
PCT/US 01/12157

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/00 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, PAJ, INSPEC, EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 751 813 A (DORENBOS DAVID) 12 May 1998 (1998-05-12) column 2, line 5 - line 67 column 6, line 35 - line 62 figures 1,3,4	1-73
A	US 5 812 671 A (ROSS JR ROBERT C) 22 September 1998 (1998-09-22) the whole document	1-73
A	MENEZES, OORSCHOT, VANSTONE: "HANDBOOK OF APPLIED CRYPTOGRAPHY" HANDBOOK OF APPLIED CRYPTOGRAPHY, XX, XX, October 1996 (1996-10), XP002182401 page 497 -page 498 page 506 -page 508	1-73

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 November 2001	27/11/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Carnerero Álvaro, F

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

In. ational Application No
PCT/US 01/12157

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
US 5751813 A	12-05-1998	AU	3877997 A	19-11-1997
		BR	9702187 A	29-06-1999
		CA	2224661 A1	06-11-1997
		EP	0882340 A1	09-12-1998
		IL	122438 A	31-10-2000
		JP	11509075 T	03-08-1999
		PL	324266 A1	11-05-1998
		RU	2147792 C1	20-04-2000
		WO	9741661 A2	06-11-1997
US 5812671 A	22-09-1998	EP	0906677 A2	07-04-1999
		WO	9802989 A1	22-01-1998

THIS PAGE BLANK (USPTO)